





# **54Mbps Wireless 4-port Router with built-in ADSL Modem**

---

From SMC's line of award-winning connectivity solutions

**SMC<sup>®</sup>**

**Networks**

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

December 2003 R.01 F1.0

Information furnished is believed to be accurate and reliable. However, no responsibility is assumed by our company for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of our company. We reserve the right to change specifications at any time without notice.

Copyright © 2003 by  
SMC Networks, Inc.  
38 Tesla  
Irvine, CA 92618  
All rights reserved.

**Trademarks:**

SMC is a registered trademark; and Barricade is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

# LIMITED WARRANTY

**Limited Warranty Statement:** SMC Networks, Inc. (“SMC”) warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime\* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an “Active” SMC product. A product is considered to be “Active” while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an “Active” SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:

[http://www.smc.com/index.cfm?action=customer\\_service\\_warranty](http://www.smc.com/index.cfm?action=customer_service_warranty).

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

## LIMITED WARRANTY

**WARRANTIES EXCLUSIVE:** IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

**LIMITATION OF LIABILITY:** IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

\* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.  
38 Tesla  
Irvine, CA 92618

# COMPLIANCES

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

**FCC Caution:** To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

## IMPORTANT STATEMENT FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm (8 in) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## FCC - Part 68

This equipment complies with Part 68 of the FCC rules. This equipment comes with a label attached to it that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC jacks: RJ-11C.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact our company at the numbers shown on back of this manual for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

No repairs may be done by the customer.

This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

When programming and/or making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in off-peak hours such as early morning or late evenings.

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device to send any message via a telephone facsimile machine unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or such business, other entity, or individual.

In order to program this information into your facsimile, refer to your communications software user manual.

## Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie.

## Australia AS/NZS 3548 (1995) - Class B



ACN 096 592 442

SMC contact for products in Australia is:

SMC-Australia  
L9, 123 Epping Rd.,  
North Ryde, NSW Australia  
Phone: 61-2-88757887  
Fax: 61-2-88757777

## EC Conformance Declaration

SMC contact for these products in Europe is:

SMC Networks Europe,  
Edificio Conata II,  
Calle Frutuós Gelabert 6-8, 2o, 4a,  
08970 - Sant Joan Despí,  
Barcelona, Spain.

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN 300 328-1 December 2001 V1.3.1

EN 300 328-2 December 2001 V1.2.1

EN 301 489-1 September 2001 V1.4.1

EN 301 489-17 September 2000 V1.2.1

EN 60950 January 2000



## Safety Compliance

### Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlusßsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlusßleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
  - a. Netzkabel oder Netzstecker sind beschädigt.
  - b. Flüssigkeit ist in das Gerät eingedrungen.
  - c. Das Gerät war Feuchtigkeit ausgesetzt.
  - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
  - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
  - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden. Für einen Nennstrom bis 6 A und einem Gerätegewicht größer 3 kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75 mm<sup>2</sup> einzusetzen.

Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70 dB(A) oder weniger.

# TABLE OF CONTENTS

<b>1</b>	<b>Introduction . . . . .</b>	<b>1-1</b>
	About the Barricade . . . . .	1-1
	Features and Benefits . . . . .	1-1
	Applications . . . . .	1-2
<b>2</b>	<b>Installation . . . . .</b>	<b>2-1</b>
	Package Contents . . . . .	2-1
	System Requirements . . . . .	2-2
	Hardware Description . . . . .	2-2
	LED Indicators . . . . .	2-4
	ISP Settings . . . . .	2-5
	Connect the System . . . . .	2-5
	Connect the ADSL Line . . . . .	2-5
	Phone Line Configuration . . . . .	2-6
	Connect the Power Adapter . . . . .	2-8
<b>3</b>	<b>Configuring Client PC . . . . .</b>	<b>3-1</b>
	TCP/IP Configuration . . . . .	3-2
	Windows 98/Me . . . . .	3-2
	Disable HTTP Proxy . . . . .	3-4
	Obtain IP Settings from Your ADSL Router . . . . .	3-6
	Windows NT 4.0 . . . . .	3-7
	Disable HTTP Proxy . . . . .	3-9
	Obtain IP Settings from Your Barricade . . . . .	3-9
	Windows 2000 . . . . .	3-11
	Disable HTTP Proxy . . . . .	3-12
	Obtain IP Settings from Your Barricade . . . . .	3-12
	Windows XP . . . . .	3-14
	Disable HTTP Proxy . . . . .	3-14
	Obtain IP Settings from Your Barricade . . . . .	3-14
	Configuring Your Macintosh Computer . . . . .	3-16
	Disable HTTP Proxy . . . . .	3-17

<b>4</b>	<b>Configuring the Barricade</b>	<b>4-1</b>
	Navigating the Management Interface	4-2
	Making Configuration Changes	4-2
	Setup Wizard	4-3
	Time Zone	4-3
	Parameter Setting	4-4
	Confirm	4-5
	Parameter Setting - Country or ISP Not Listed	4-7
	ISP use RFC1483 Bridging - Parameter Setting	4-8
	ISP use PPPoE - Parameter Setting	4-10
	ISP use PPPoA - Parameter Setting	4-11
	ISP use RFC1483 Routing - Parameter Setting	4-12
	Advanced Setup	4-13
	System	4-15
	WAN	4-19
	LAN	4-24
	Wireless	4-25
	NAT	4-31
	Routing	4-35
	Firewall	4-40
	SNMP	4-51
	ADSL	4-53
	DDNS	4-57
	UPnP	4-58
	Tools	4-59
	Status	4-62
	Finding the MAC address of a Network Card	4-64
	Windows 98/ME	4-64
	Windows NT4/2000/XP	4-64
	Macintosh	4-64
	Linux	4-64

<b>A</b>	<b>Troubleshooting</b> . . . . .	<b>A-1</b>
<b>B</b>	<b>Cables</b> . . . . .	<b>B-1</b>
	Ethernet Cable . . . . .	B-1
	Specifications . . . . .	B-1
	Wiring Conventions . . . . .	B-1
	RJ-45 Port Connection . . . . .	B-2
	Pin Assignments . . . . .	B-3
	ADSL Cable . . . . .	B-5
	Specifications . . . . .	B-5
	Wiring Conventions . . . . .	B-5
<b>C</b>	<b>Specifications</b> . . . . .	<b>C-1</b>

## *TABLE OF CONTENTS*

# CHAPTER 1

## INTRODUCTION

---

Congratulations on your purchase of the ADSL Barricade™, hereafter referred to as the "Barricade". We are proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet in the most secure way, this router provides a convenient and powerful solution.

### About the Barricade

The Barricade provides Internet access to multiple users by sharing a single-user account. Support is provided for both wired and wireless devices. New technology provides wireless security via Wired Equivalent Privacy (WEP) encryption and MAC address filtering. It is simple to configure and can be up and running in minutes.

### Features and Benefits

- Internet connection to an ADSL modem via an RJ-11 ADSL port
- Local network connection via four 10/100 Mbps Ethernet ports
- On-board IEEE 802.11g wireless network adapter
- DHCP for dynamic IP configuration, and DNS for domain name mapping

- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT
- NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as web, FTP, e-mail, and Telnet)
- VPN pass-through (IPSec-ESP Tunnel mode, L2TP, PPTP)
- User-definable application sensing tunnel supports applications requiring multiple connections
- Easy setup through a web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications

## Applications

Many advanced networking features are provided by the Barricade:

- **Wireless and Wired LAN**

The Barricade provides connectivity to 10/100 Mbps devices, and wireless IEEE 802.11g compatible devices, making it easy to create a network in small offices or homes.

- **Internet Access**

This device supports Internet access through an ADSL connection. Since many DSL providers use PPPoE or PPPoA to establish communications with end users, the Barricade includes built-in clients for these protocols, eliminating the need to install these services on your computer.

- **Shared IP Address**

The Barricade provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the web at the same time.

- **Virtual Server**

If you have a fixed IP address, you can set the Barricade to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the Barricade can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

- **DMZ Host Support**

Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.

- **Security**

The Barricade supports security features that deny Internet access to specified users, or filter all requests for specific services that the administrator does not want to serve. The Barricade's firewall also blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. WEP (Wired Equivalent Privacy), SSID, and MAC filtering provide security over the wireless network.



- **Virtual Private Network (VPN)**

The Barricade supports three of the most commonly used VPN protocols — PPTP, L2TP, and IPSec. These protocols allow remote users to establish a secure connection to their corporate network. If your service provider supports VPNs, then these protocols can be used to create an authenticated and encrypted tunnel for passing secure data over the Internet (i.e., a traditionally shared data network). The VPN protocols supported by the Barricade are briefly described below.

- Point-to-Point Tunneling Protocol — Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs.
- L2TP merges the best features of PPTP and L2F — Like PPTP, L2TP requires that the ISP's routers support the protocol.
- IP Security — Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

# CHAPTER 2

## INSTALLATION

---

Before installing the ADSL Barricade™, verify that you have all the items listed under the Package Contents list. If any of the items are missing or damaged, contact your local distributor. Also be sure that you have all the necessary cabling before installing the Barricade. After installing the Barricade, refer to “Configuring the Barricade” on page 4-1.

### Package Contents

After unpacking the Barricade, check the contents of the box to be sure you have received the following components:

- Barricade ADSL Router (SMC7804WBRA)
- Power adapter
- One CAT-5 Ethernet cable (RJ-45)
- Telephone patch cable (RJ-11)
- Quick install guide
- Documentation CD

Immediately inform your dealer in the event of any incorrect, missing, or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

## System Requirements

You must meet the following minimum requirements:

- ADSL line installed by your Internet Service Provider.
- A PC using a fixed IP address or dynamic IP address assigned via DHCP, as well as a gateway server address and DNS server address from your service provider.
- A computer equipped with a 10/100 Mbps network adapter, a USB-to-Ethernet converter or an IEEE 802.11g wireless network adapter.
- TCP/IP network protocols installed on each PC that will access the Internet.
- A Java-enabled web browser, such as Microsoft Internet Explorer 5.0 or above installed on one PC at your site for configuring the Barricade.

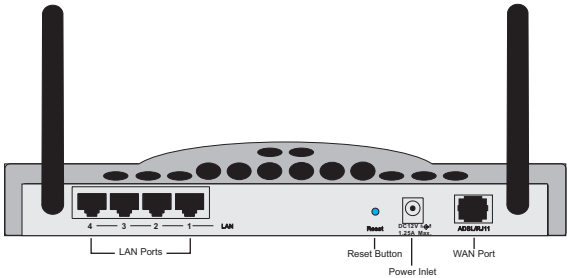
## Hardware Description

The Barricade contains an integrated ADSL modem and connects to the Internet or to a remote site using its RJ-11 WAN port. It can be connected directly to your PC or to a local area network using any of the four Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full-rate ADSL provides up to 8 Mbps downstream and 640 kbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 kbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports and 54 Mbps over the built-in wireless network adapter.

The Barricade includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. It also provides the following ports on the rear panel:



**Figure 2-1. Rear Panel**

Item	Description
LAN Ports	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).
Reset Button	Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see “Reset” on page 4-61.
Power Inlet	Connect the included power adapter to this inlet. <b>Warning:</b> Using the wrong type of power adapter may damage the Barricade.
ADSL Port	WAN port (RJ-11). Connect your ADSL line to this port.

LED Indicators

The power and port LED indicators on the front panel are illustrated by the following figure and table.

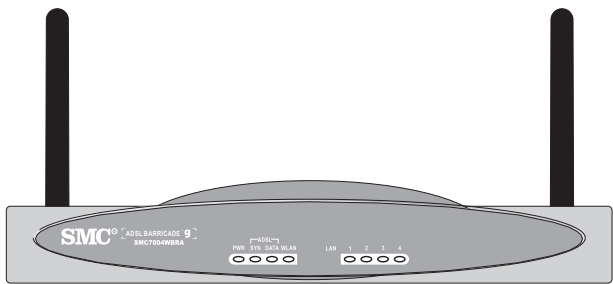


Figure 2-2. Front Panel

LED	Status	Description
PWR	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
ADSL SYN	On	ADSL connection is functioning correctly.
	Flashing	The Barricade is establishing an ADSL link.
	Off	ADSL connection is not established.
ADSL DATA	Flashing	The indicated ADSL port is sending or receiving data.
	Off	No data is being transferred.
WLAN	Flashing	The WLAN port is sending or receiving data.
LAN (4 LEDs)	On	Ethernet connection is established.
	Flashing	The indicated LAN port is sending or receiving data.
	Off	There is no LAN connection on the port.

## **ISP Settings**

Please collect the following information from your ISP before setting up the Barricade:

- ISP account user name and password
- Protocol, encapsulation and VPI/VCI circuit numbers
- DNS server address
- IP address, subnet mask and default gateway (for fixed IP users only)

## **Connect the System**

The Barricade can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the Barricade away from any heating devices.
- Do not place the Barricade in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the Barricade.

## **Connect the ADSL Line**

Connect the supplied RJ-11 cable from the ADSL Microfilter/Splitter to the ADSL port on your Barricade. When inserting an ADSL RJ-11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

## Phone Line Configuration

### Installing a Full-Rate Connection

If you are using a full-rate (G.dmt) connection, your service provider will attach the outside ADSL line to a data/voice splitter. In this case you can connect your phones and computer directly to the splitter as shown below:

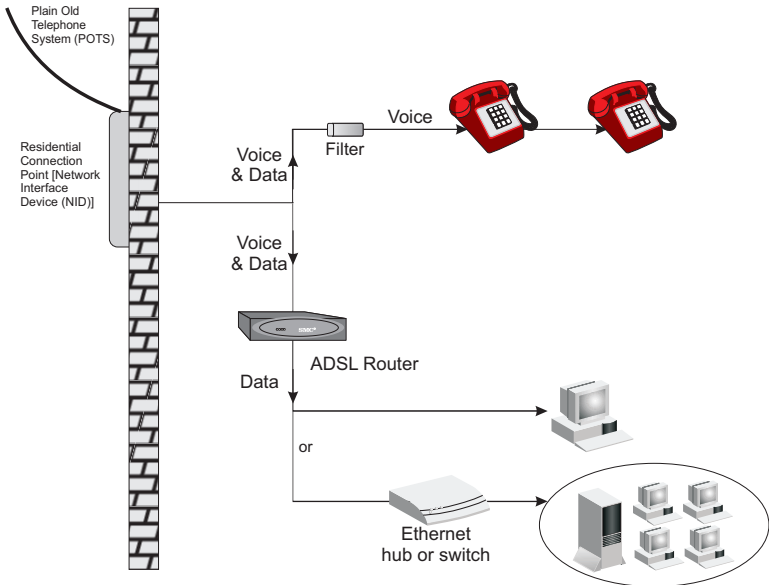


Figure 2-3. Installing with a Splitter

### Installing a Splitterless Connection

If you are using a splitterless (G.lite) connection, then your service provider will attach the outside ADSL line directly to your phone system. In this case you can connect your phones and computer directly to the incoming ADSL line, but you will have to add low-pass filters to your phones as shown below:

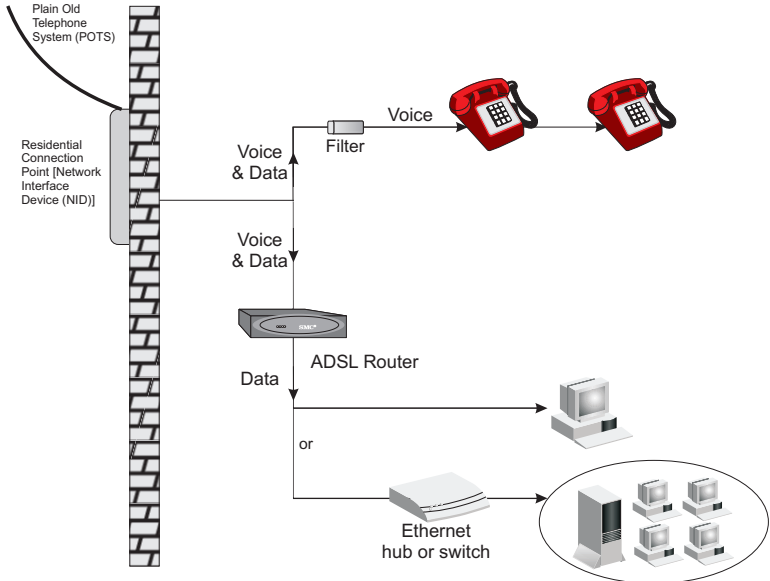


Figure 2-4. Installing without a Splitter



### **Attach to Your Network Using Ethernet Cabling**

The four LAN ports on the Barricade auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half duplex or full duplex.

Use RJ-45 cables to connect any of the four LAN ports on the Barricade to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the Barricade to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated.

**Warning:** Do not plug a phone jack connector into an RJ-45 port. This may damage the Barricade.

- Notes:**
1. Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Use Category 3, 4, or 5 for connections that operate at 10 Mbps, and Category 5 for connections that operate at 100 Mbps.
  2. Make sure each twisted-pair cable length does not exceed 100 meters (328 feet).

### **Connect the Power Adapter**

Plug the power adapter into the power socket on the rear of the Barricade, and the other end into a power outlet.

Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to “Troubleshooting” on page A-1.

In case of a power input failure, the Barricade will automatically restart and begin to operate once the input power is restored.

# CHAPTER 3

## CONFIGURING CLIENT PC

---

After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Barricade.

See:

“Windows 98/Me” on page 3-2

“Windows NT 4.0” on page 3-7

“Windows 2000” on page 3-11

“Windows XP” on page 3-14

or

“Configuring Your Macintosh Computer” on page 3-16

depending on your operating system.

## TCP/IP Configuration

To access the Internet through the Barricade, you must configure the network settings of the computers on your LAN to use the same IP subnet as the Barricade. The default IP settings for the Barricade are:

IP Address: 192.168.2.1

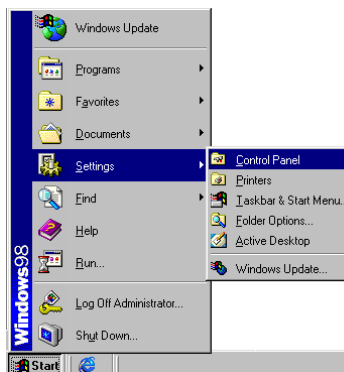
Subnet Mask: 255.255.255.0

**Note:** These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Barricade's web configuration interface in order to make the required changes. (See "Configuring the Barricade" on page 4-1 for instruction on configuring the Barricade.)

## Windows 98/Me

You may find that the instructions in this section do not exactly match your version of Windows. This is because these steps and screen shots were created from Windows 98. Windows Millennium Edition is similar, but not identical, to Windows 98.

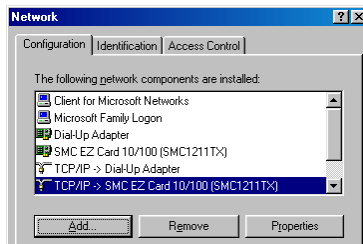
1. On the Windows desktop, click Start/Settings/Control Panel.



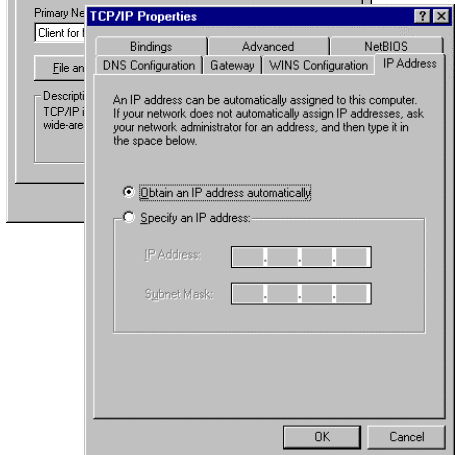
2. In Control Panel, double-click the Network icon.



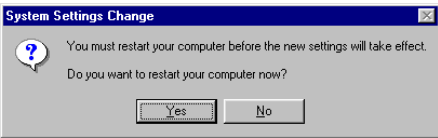
3. In the Network window, under the Configuration tab, double-click the TCP/IP item listed for your network card.



4. In the TCP/IP window, select the IP Address tab. If “Obtain an IP address automatically” is already selected, your computer is already configured for DHCP. If not, select this option.



- 5. Windows may need your Windows 95/98/Me CD to copy some files. After it finishes copying, it will prompt you to restart your system. Click Yes and your computer will restart.




**TCP/IP Configuration Setting**

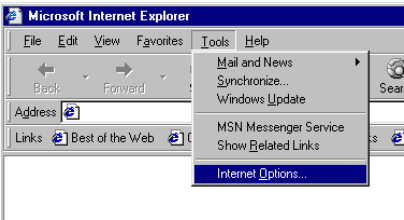
Primary DNS Server	_____
Secondary DNS Server	_____
Default Gateway	_____
Host Name	_____

**Disable HTTP Proxy**

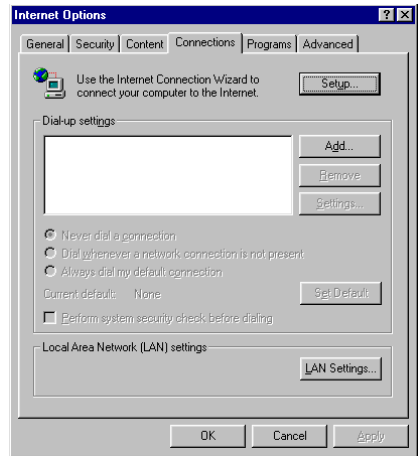
You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. The following steps are for Internet Explorer.

**Internet Explorer**

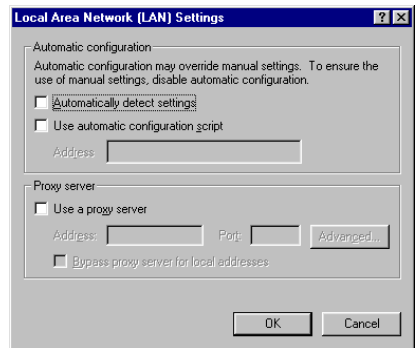
- 1. Open Internet Explorer.
- 2. Click the Stop  button, then click Tools/Internet Options.



3. In the Internet Options window, click the Connections tab. Next, click the LAN Settings... button.



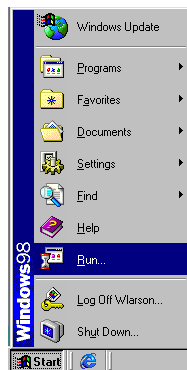
4. Clear all the check boxes.
5. Click OK, and then click OK again to close the Internet Options window.



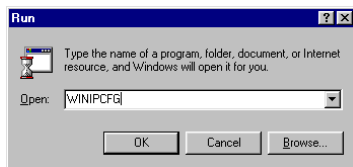
## Obtain IP Settings from Your ADSL Router

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can also verify that you have configured your computer correctly.

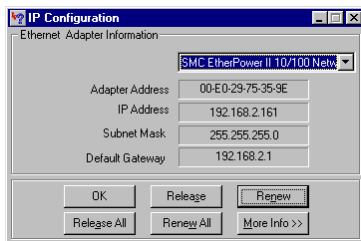
1. On the Windows desktop, click Start/Run...



2. Type "WINIPCFG" and click OK.  
It may take a second or two for the IP Configuration window to appear.

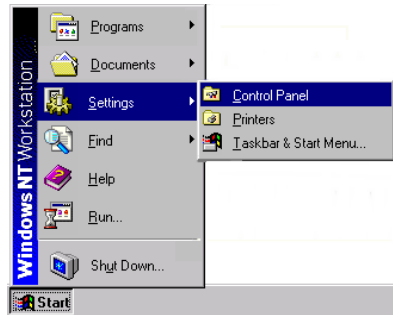


3. In the IP Configuration window, select your network card from the drop-down menu. Click Release and then click Renew. Verify that your IP address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning. Click OK to close the IP Configuration window.

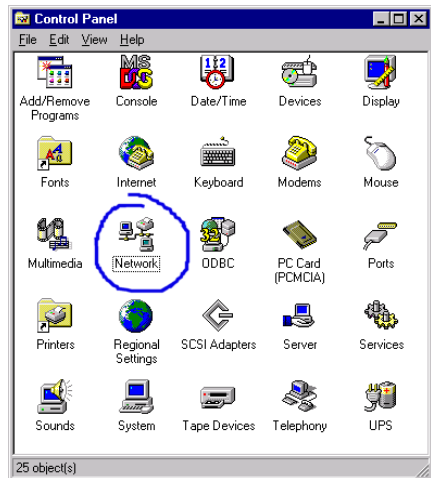


## Windows NT 4.0

1. On the Windows desktop, click Start/Settings/Control Panel.

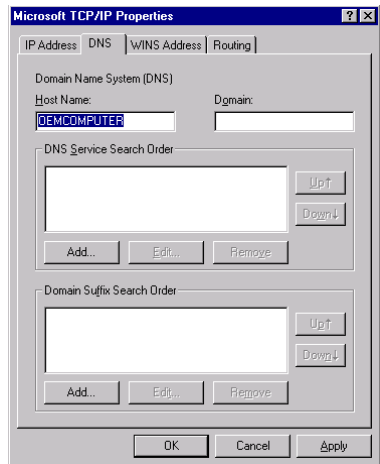
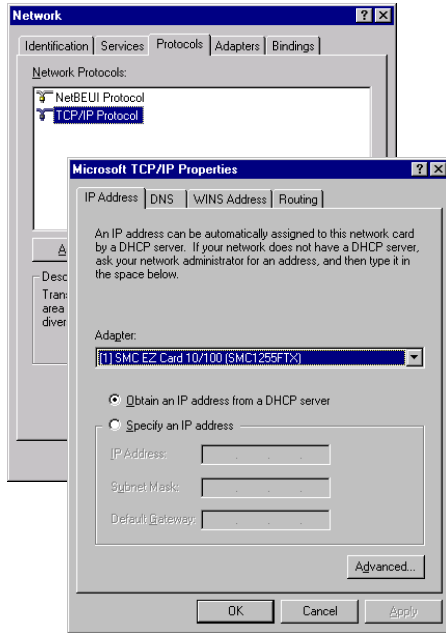


2. Double-click the Network icon.





3. In the Network window, Select the Protocols tab. Double-click TCP/IP Protocol.
4. When the Microsoft TCP/IP Properties window open, select the IP Address tab.
5. In the Adapter drop-down list, be sure your Ethernet adapter is selected.
6. If “Obtain an IP address automatically” is already selected, your computer is already configured for DHCP. If not, select this option and click “Apply.”
7. Click the DNS tab to see the primary and secondary DNS servers. Record these values, and then click “Remove.” Click “Apply”, and then “OK.”



8. Windows may copy some files, and will then prompt you to restart your system. Click Yes and your computer will shut down and restart.

### **TCP/IP Configuration Setting**

Default Gateway	____.____.____.____
Primary DNS Server	____.____.____.____
Secondary DNS Server	____.____.____.____
Host Name	____.____.____.____

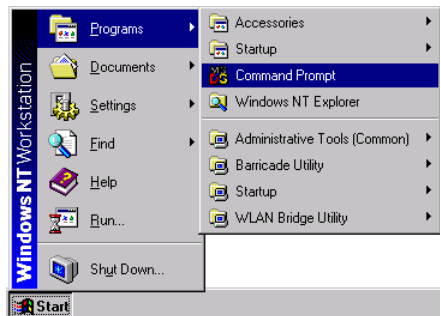
## **Disable HTTP Proxy**

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. Determine which browser you use and refer to “Internet Explorer” on page 3-4.

## **Obtain IP Settings from Your Barricade**

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you will verify that you have configured your computer correctly.

1. On the Windows desktop, click Start/Programs/Command Prompt.

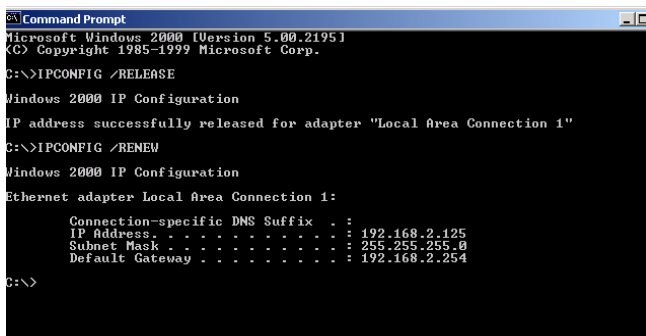


## CONFIGURING CLIENT PC

2. In the Command Prompt window, type “IPCONFIG /RELEASE” and press the ENTER key.



3. Type “IPCONFIG /RENEW” and press the ENTER key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.254**. These values confirm that your Barricade is functioning.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"

C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 1:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.125
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.254

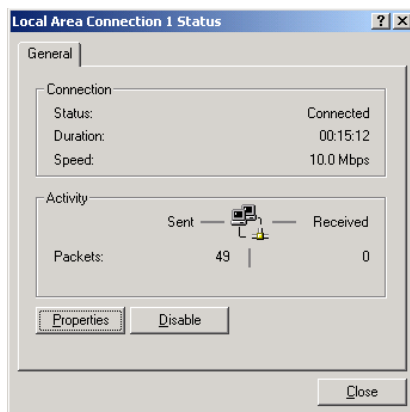
C:\>
```

4. Type “EXIT” and press the ENTER key to close the Command Prompt window.

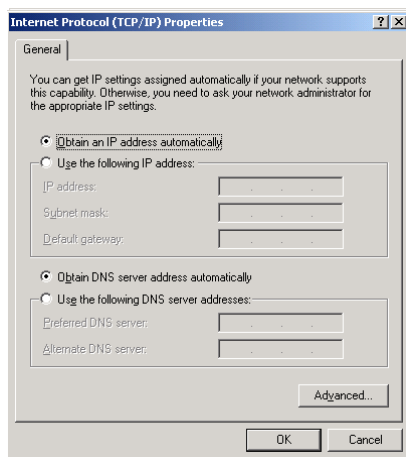
Your computer is now configured to connect to the Barricade.

# Windows 2000

1. On the Windows desktop, click Start/Settings/Network and Dial-Up Connections.
2. Click the icon that corresponds to the connection to your Barricade.
3. The connection status screen will open. Click Properties.



4. Double-click Internet Protocol (TCP/IP).
5. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. If not, select this option.



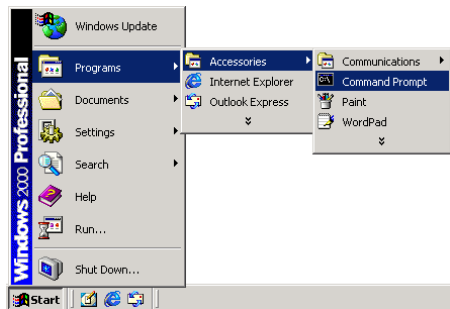
## Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. Determine which browser you use and refer to “Internet Explorer” on page 3-4.

## Obtain IP Settings from Your Barricade

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly.

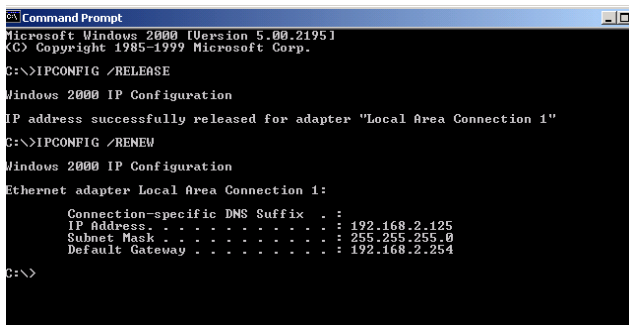
1. On the Windows desktop, click Start/Programs/Accessories/Command Prompt.



2. In the Command Prompt window, type “IPCONFIG/RELEASE” and press the ENTER key.



3. Type "IPCONFIG /RENEW" and press the ENTER key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.254**. These values confirm that your ADSL Router is functioning.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"

C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 1:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.125
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.254

C:\>
```

4. Type "EXIT" and press the ENTER key to close the Command Prompt window.

Your computer is now configured to connect to the Barricade.

## Windows XP

1. On the Windows desktop, click Start/Control Panel.
2. In the Control Panel window, click Network and Internet Connections.
3. The Network Connections window will open. Double-click the connection for this device.
4. On the connection status screen, click Properties.
5. Double-click Internet Protocol (TCP/IP).
6. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. If not, select this option.

### Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. Determine which browser you use and refer to “Internet Explorer” on page 3-4.

### Obtain IP Settings from Your Barricade

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly.

1. On the Windows desktop, click Start/Programs/Accessories/Command Prompt.

2. In the Command Prompt window, type “IPCONFIG/RELEASE” and press the ENTER key.
3. Type “IPCONFIG /RENEW” and press the ENTER key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.254**. These values confirm that your ADSL router is functioning.

Type “EXIT” and press the ENTER key to close the Command Prompt window.


Your computer is now configured to connect to the Barricade.

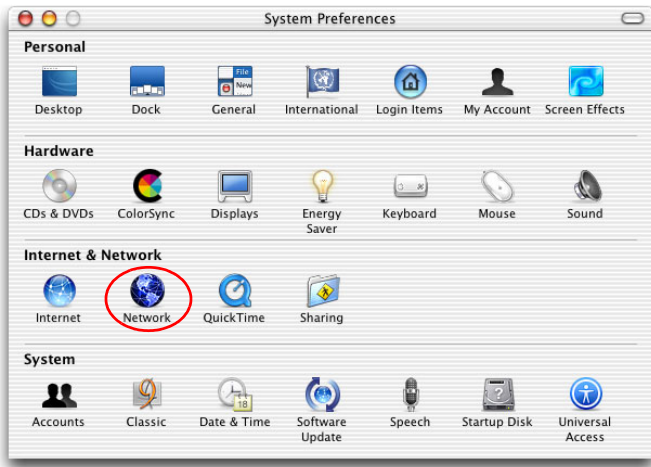
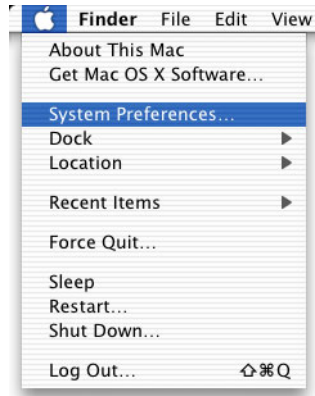


# Configuring Your Macintosh Computer

You may find that the instructions here do not exactly match your operating system. This is because these steps and screenshots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

1. Pull down the Apple Menu  Click System Preferences
2. Double-click the Network icon in the Systems Preferences window.



3. If “Using DHCP Server” is already selected in the Configure field, your computer is already configured for DHCP. If not, select this Option.



4. Your new settings are shown on the TCP/IP tab. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning.
5. Close the Network window.

Now your computer is configured to connect to the Barricade.

## Disable HTTP Proxy

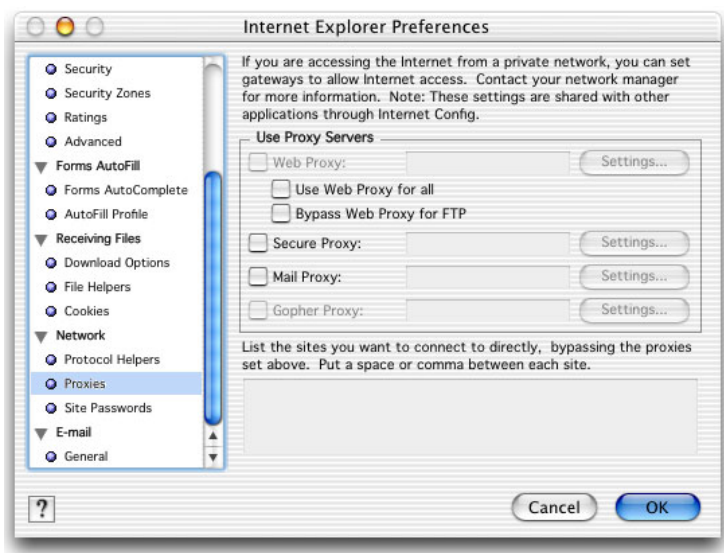
You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. The following steps are for Internet Explorer.

### Internet Explorer

1. Open Internet Explorer and click the Stop button. Click Explorer/Preferences.
2. In the Internet Explorer Preferences window, under Network, select Proxies.



3. Uncheck all check boxes and click OK.



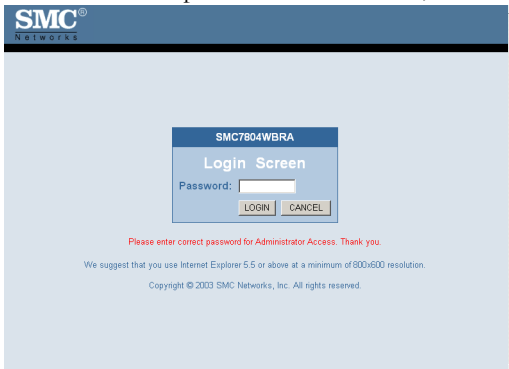
# CHAPTER 4

## CONFIGURING THE BARRICADE

---

After you have configured TCP/IP on a client computer, you can configure the Barricade using Internet Explorer 5.0 or above.

To access the Barricade's management interface, enter the default IP address of the Barricade in your web browser: `http://192.168.2.1`. Enter the default password: "smcadmin", and click "LOGIN".



## Navigating the Management Interface



The Barricade's management interface consists of a Setup Wizard and an Advanced Setup section.



**Setup Wizard:** Use the Setup Wizard if you want to quickly set up the Barricade. Go to “Setup Wizard” on page 4-3.

**Advanced Setup:** Advanced Setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, virtual server setup, virtual DMZ host, as well as other functions. Go to “Advanced Setup” on page 4-13.

## Making Configuration Changes

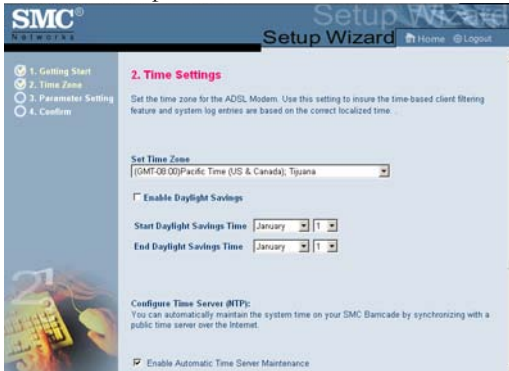
Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, click the “APPLY”  or “NEXT”  button at the bottom of the page to enable the new setting.

**Note:** To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 is configured as follows: Under the menu Tools/Internet Options/General/Temporary Internet Files/Settings, the setting for “Check for newer versions of stored pages” should be “Every visit to the page.”

# Setup Wizard

## Time Zone

Click on “Setup Wizard”. The first item in the Setup Wizard is Time Zone.



For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop-down list. If your area requires it, check to enable the clock for daylight saving changes, and enter the Daylight Savings Time start and end dates for your location.

If you want to automatically synchronize the ADSL router with a public time server, check the box to enable Enable Automatic Time Server Maintenance. Select the desired servers from the drop down menu.

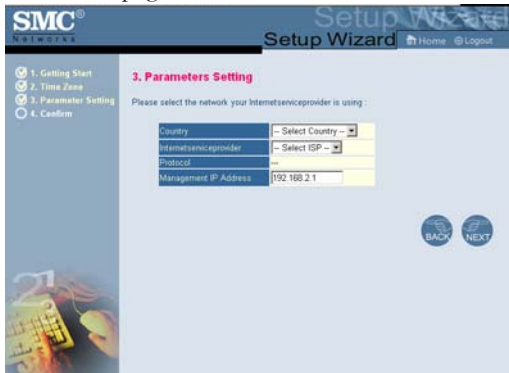
Click “NEXT” to continue.

**Note:** Units sold in the United States are configured by default to use only radio channels 1-11 as defined by FCC regulations. Units sold in other countries are configured by default without a country code (i.e., 99). Setting the country code restricts operation of the device to the radio channels permitted for the wireless networks in the specified country.

## Parameter Setting

Select your Country and Internet Service Provider. This will automatically configure the Barricade with the correct Protocol, Encapsulation and VPI/VCI settings for your ISP.

If your Country or Internet Service Provider is not listed you will need to manually enter settings. Go to “Parameter Setting - Country or ISP Not Listed” on page 4-7 in the manual.



SMC®  
Setup Wizard

1. Getting Start  
2. Time Zone  
3. Parameter Setting  
4. Confirm

**3. Parameters Setting**

Please select the network your Internet service provider is using :

Country	- Select Country ->
Internet service provider	- Select ISP ->
Protocol	-
Management IP Address	192.168.2.1

BACK NEXT

If your ISP uses Protocols PPPoA or PPPoE you will need to enter the username, password and DNS Server address supplied by your ISP.

If your ISP uses Protocol RFC1483 Routed you will need to enter the IP address, Subnet Mask, Default Gateway and DNS Server address supplied by your ISP.

**Note:** By default 192.168.2.1 is set for the DNS Server address, this needs to be changed to reflect your ISP’s DNS Server address.

Click “NEXT” to continue.

## Confirm

The Confirm page shows a summary of the configuration parameters. Check ADSL operation mode (WAN), Network Layer Parameters (WAN) and ISP parameters are correct.



Parameter	Description
<b>ADSL Operation Mode (WAN)</b>	
ISP	The type of ISP you have selected.
Protocol	Indicates the protocol used.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI).
AAL5 Encapsulation	Shows the packet encapsulation type. Go to page 4-20 for a detailed description.
<b>Network Layer Parameters (WAN)</b>	
IP Address	WAN IP address (only displayed if you have static IP).
Subnet Mask	WAN subnet mask (only displayed if you have static IP).
Default Gateway	WAN gateway (only displayed if you have static IP).
DNS Server	The IP address of the DNS server.
<b>ISP Parameters</b>	
Username	The ISP assigned user name.
Password	The password (hidden).



Parameter	Description
DHCP Parameters	
Function	Shows the DHCP function is enabled or disabled.
Default Gateway	LAN IP address of the Barricade.
Subnet Mask	The network subnet mask.
Name Server 1	Primary DNS server IP address.
Name Server 2	Alternate DNS server IP address.
Start IP Address	Start IP address of DHCP assigned IP addresses.
Number of IP	Number of IP addresses available for assignment by the DHCP server.

If the parameters are correct, click “APPLY” to save these settings.

Your Barricade is now set up. Go to “Troubleshooting” on page A-1 if you cannot make a connection to the Internet.

## Parameter Setting - Country or ISP Not Listed

If your Country or Internet Service Provider is not listed select “Others”. This will allow you to manually configure your ISP settings.

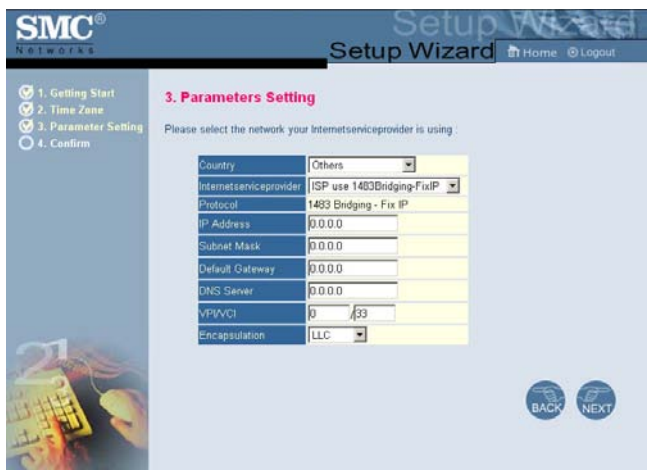
For manual configuration you will need to know the Protocol, DNS Server, Encapsulation and VPI/VCI settings used by your ISP. If you have a Static IP address you will also need to know the IP address, Subnet Mask and Gateway address. Please contact your ISP for these details if you do not already have them.

After selecting “Others” you will be required to select what Protocol your ISP uses from the “Internet Service Provider” drop down list.

ISP use RFC1483 Bridging - Parameter Setting

Enter the RFC1483 Bridging settings provided by your ISP.

**Note:** You have three different bridging modes to select from:  
 RFC1483 Bridging - Select this option if you want the Barricade to be transparent and pass the public IP address to a single PC, Server or Firewall.  
 RFC1483 Bridging DHCP - Select this option if you want to share the connection for multiple PC's (most common setting).  
 RFC1483 Bridging FixIP - Select this option if your ISP has given you a static IP address.



Parameter	Description
IP Address	Enter IP address provided by your ISP (only displayed with FixIP).
Subnet Mask	Enter the subnet mask address provided by your ISP (only displayed with FixIP).
Default Gateway	Enter the gateway address provided by your ISP (only displayed with FixIP).
DNS Server	Enter the Domain Name Server address.

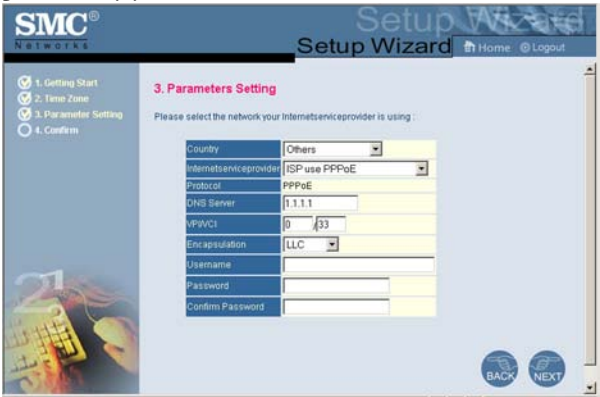
<b>Parameter</b>	<b>Description</b>
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down list.

Click “NEXT” to continue to the “Confirm” settings page.

Go to “Confirm” on page 4-5 in the manual for details about the “Confirm” settings page.

ISP use PPPoE - Parameter Setting

Enter the PPPoE (Point-to-Point Protocol over Ethernet) settings provided by your ISP.



Parameter	Description
DNS Server	Enter the ISP Domain Name Server address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down list.
Username	Enter the ISP assigned user name.
Password	Enter your password.
Confirm Password	Confirm your password.

Click “NEXT” to continue to the “Confirm” settings page.

Go to “Confirm” on page 4-5 in the manual for details about the “Confirm” settings page.

## ISP use PPPoA - Parameter Setting

Enter the PPPoA (Point-to-Point Protocol over ATM) settings provided by your ISP.

**SMC® NETWORKS** Setup Wizard Home Logout

**3. Parameters Setting**

Please select the network your Internet service provider is using :

Country: Others

Internet Service Provider: ISP use PPPoA

Protocol: PPPoA

DNS Server: 1.1.1.1

VPI/VCI: 0 / 32

Encapsulation: VC MLK

Username:

Password:

Confirm Password:

BACK NEXT

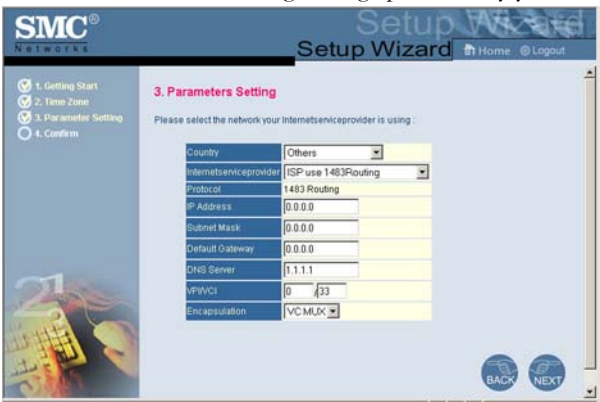
Parameter	Description
DNS Server	Enter the ISP Domain Name Server address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down list.
Username	Enter the ISP assigned user name.
Password	Enter your password.
Confirm Password	Confirm your password.

Click “NEXT” to continue to the “Confirm” settings page.

Go to “Confirm” on page 4-5 in the manual for details about the “Confirm” settings page.

ISP use RFC1483 Routing - Parameter Setting

Enter the RFC1483 Routing settings provided by your ISP.



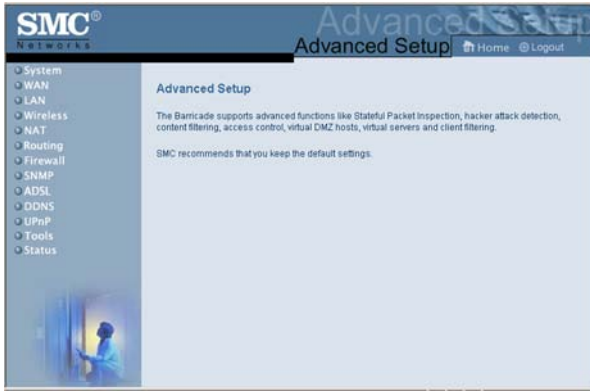
Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the Domain Name Server address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down list.

Click “NEXT” to continue to the “Confirm” settings page.

Go to “Confirm” on page 4-5 in the manual for details about the “Confirm” settings page.

## Advanced Setup

Click on the Advanced Setup picture. The left-hand side displays the main menu and the right-hand side shows descriptive information.



The advanced management interface contains 13 main menu items as described in the following table.

Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the Barricade remotely.
WAN	Specifies the Internet connection settings.
LAN	Sets the TCP/IP configuration for the Barricade LAN interface and DHCP clients.
Wireless	Configures the radio frequency, SSID, and security for wireless communications.
NAT	Configures Address Mapping, virtual server and special applications.
Routing	Sets the routing parameters and displays the current routing table.
Firewall	Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, intruder detection, and DMZ.
SNMP	Community string and trap server settings.
ADSL	Sets the ADSL operation type and shows the ADSL status.

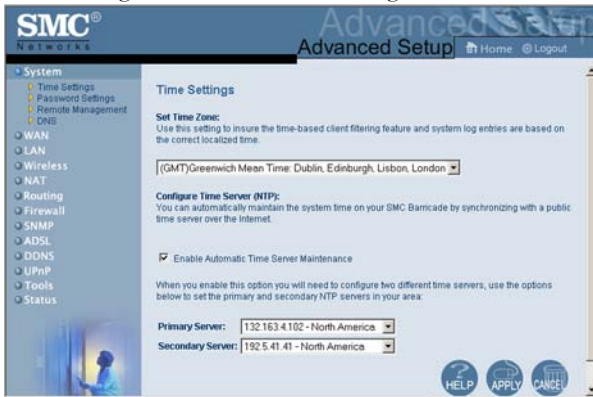


Menu	Description
DDNS	Dynamic DNS provides users on the Internet with a method to tie their domain name(s) to a Dynamic or Static IP address.
UPnP	Allows you to enable or disable the Universal Plug and Play function.
Tools	Contains options to backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system.
Status	Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and firewall information. Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number. Shows the security and DHCP client log.

## System

### Time Settings

Select your local time zone from the drop down list. This information is used for log entries and client filtering.



For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop down list.

If you want to automatically synchronize the ADSL router with a public time server, check the box to Enable Automatic Time Server Maintenance. Select the desired servers from the drop down menu.

## Password Settings

Use this page to change the password for accessing the management interface of the Barricade.



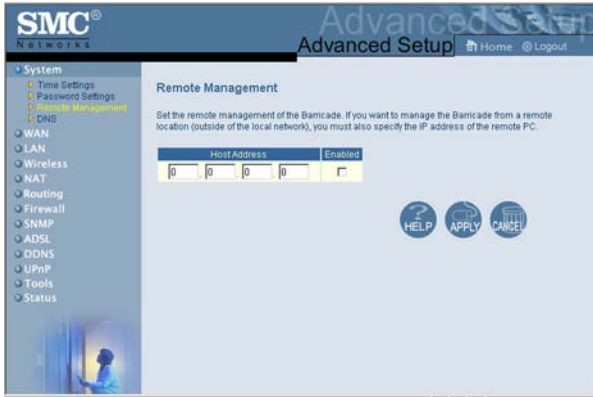
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

**Note:** If you lost the password, or you cannot gain access to the user interface, press the blue reset button on the rear panel, holding it down for at least five seconds to restore the factory defaults. The default password is “smcadmin”.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes)

## Remote Management

By default, management access is only available to users on your local network. However, you can also manage the Barricade from a remote host by entering the IP address of a remote computer on this screen. Check the Enabled check box, and enter the IP address of the Host Address and click “APPLY”.



**Note:** If you check Enable and specify an IP address of 0.0.0.0, any remote host can manage the Barricade.

For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080, for example, 212.120.68.20:8080.

DNS

Domain Name Servers (DNS) are used to map a domain name (e.g., www.smc.com) with the IP address (e.g., 64.147.25.20). Your ISP should provide the IP address of one or more Domain Name Servers. Enter those addresses on this page, and click “APPLY”.

SMC®  
Networks

Advanced Setup

Home Logout

System

- Time Settings
- Password Settings
- Remote Management
- DNS**
- WAN
- LAN
- Wireless
- NAT
- Routing
- Firewall
- SNMP
- ADSL
- DDNS
- UPnP
- Tools
- Status

DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 202.42.118.222. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

Domain Name Server (DNS) Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Secondary DNS Address (optional)	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

HELP

APPLY

CANCEL

## WAN

Specify the WAN connection parameters provided by your Internet Service Provider (ISP).

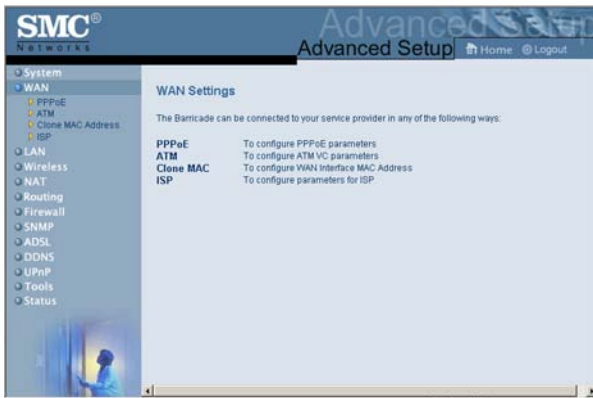
The Barricade can be connected to your ISP in one of the following ways:

PPPoE

ATM

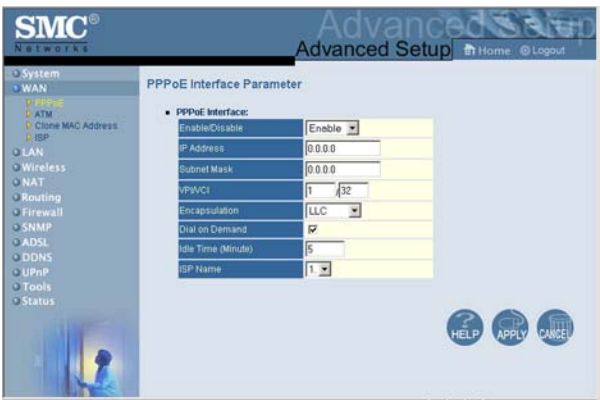
Clone MAC

ISP



PPPoE

Enter the PPPoE (Point-to-Point over Ethernet) parameters here.



Parameter	Description
Enable/Disable	Enables/disables the PPPoE function.
IP Address	If your IP address is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your ISP supplied static IP address here.
Subnet Mask	If your subnet mask is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your subnet mask here.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI).
Encapsulation	Specifies how to handle multiple protocols at the ATM transport layer. <ul style="list-style-type: none"><li>VC-MUX: Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead.</li><li>LLC: Point-to-Point Protocol over ATM Logical Link Control (LLC) allows multiple protocols running over one virtual circuit (using slightly more overhead).</li></ul>
Dial on demand	Check this box to automatically connect to your ISP.

Parameter	Description
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated.
ISP Name	Choose the ISP to whom this connection will apply.

## ATM

Enter ATM (Asynchronous Transfer Mode) function parameters here.

The screenshot shows the 'Advanced Setup' window for SMC Networks. The left sidebar contains a tree view with categories: System, WAN, PPPoE, ATM (selected), Clone MAC Address, ISP, LAN, Wireless, NAT, Routing, Firewall, SNMP, DDNS, UPnP, Tools, and Status. The main area is titled 'ATM Interface' and contains a configuration table:

ATM	
Protocol	1483 Bridging
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
VPI/VCI	1 / 32
Encapsulation	LLC
DHCP Client	<input type="checkbox"/>

At the bottom right of the configuration area are three buttons: HELP, APPLY, and CANCEL.

Parameter	Description
Protocol	<ul style="list-style-type: none"> <li>Disable: Disables the ATM mode.</li> <li>1483 Bridging: Bridging is a standardized layer 2 technology. It is typically used in corporate networks to extend the physical reach of a single LAN segment and increase the number of stations on a LAN without compromising performance. Bridged data is encapsulated using the RFC1483 protocol to enable data transport.</li> </ul>
IP Address	IP address of the ATM interface.
Subnet Mask	Subnet mask of the ATM interface.
Default Gateway	Default gateway of the ATM interface.
VPI/VCI	Each connection must have a unique pair of VPI/VCI settings.



Parameter	Description
Encapsulation	Specifies how to handle multiple protocols at the ATM transport layer. Go to“Encapsulation” on page 4-20, for a detailed description.
DHCP Client	Check this box if your ISP assigns an IP to clients using DHCP.

Clone MAC Address

Some ISPs require you to register your MAC address with them. If this is the case, the MAC address of the Barricade must be changed to the MAC address that you have registered with your ISP.



## ISP

Enter the Internet Service Provider (ISP) name, user name, and password for each ISP connection you have.

The screenshot shows the SMC Advanced Setup web interface. On the left is a navigation menu with categories like System, WAN, LAN, Wireless, NAT, Routing, Firewall, SNMP, ADSL, DDNS, UPnP, Tools, and Status. The 'WAN' category is expanded, showing sub-options: PPPoE, ATM, Clone MAC Address, and ISP. The 'ISP' option is selected. The main content area is titled 'ISP Parameter' and contains the instruction 'Please Enter the following Configuration Parameters:'. Below this is a section titled 'Table of current ISP pool:' which contains a table with 4 rows and 4 columns: Index, ISP Name, Username, and Password. The table is currently empty. At the bottom right of the main area are three circular buttons labeled 'HELP', 'APPLY', and 'CANCEL'.

Index	ISP Name	Username	Password
1			
2			
3			
4			

You can enter up to four sets of information here.

LAN

Use the LAN menu to configure the LAN IP address and to enable the DHCP server for dynamic client address allocation.

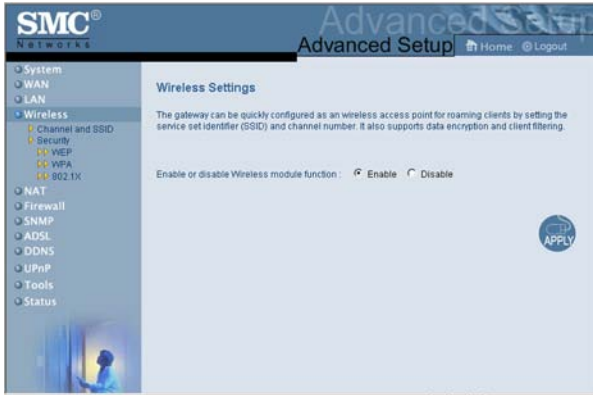


Parameter	Description
LAN IP	
IP Address	The IP address of the Barricade.
IP Subnet Mask	The subnet mask of the network.
DHCP Server	The Barricade comes with the DHCP function. To dynamically assign an IP address to client PCs, enable this function.
Lease Time	Set the IP lease time. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.
IP Address Pool	
Start IP Address	Specify the start IP address of the DHCP pool. Do not include the gateway address of the Barricade in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.2.xxx.
End IP Address	Specify the end IP address of the DHCP pool.
Domain Name	If your network uses a domain name, enter it here. Otherwise, leave this field blank.

**Note:** Remember to configure your client PCs for dynamic address allocation. (See page 3-2 for details.)

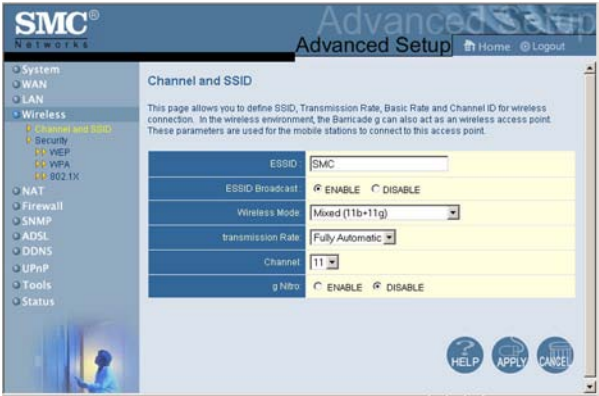
## Wireless

The Barricade also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, all you need to do is enable the wireless function, define the radio channel, the domain identifier, and the security options. Check Enable and click “APPLY”.



Channel and SSID

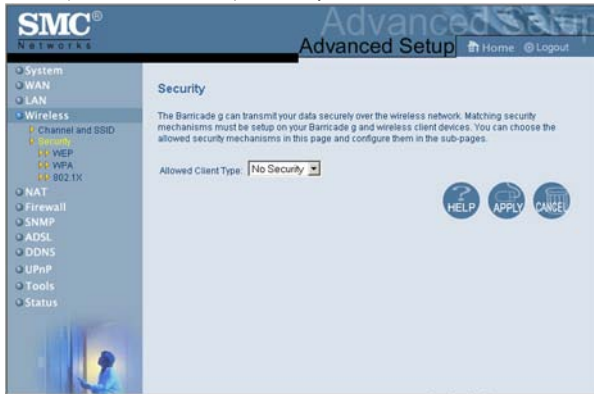
You must specify a common radio channel and SSID (Service Set ID) to be used by the Barricade Wireless Router and all of its wireless clients. Be sure you configure all of its clients to the same values.



Parameter	Description
ESSID	Extended Service Set ID. The ESSID must be the same on the Barricade and all of its wireless clients.
ESSID Broadcast	Enable or disable the broadcasting of the SSID.
Wireless Mode	This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have.
Transmission Rate	The default is Fully Automatic. The transmission rate is automatically adjusted based on the receiving data error rate. Usually the connection quality will vary depending on the distance between the wireless router and wireless adapter. You can also select a lower transmission data rate to maximize the radio communication range.
Channel	<p>The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients.</p> <p>The Barricade will automatically assign itself a radio channel, or you may select one manually.</p>
g Nitro	This is the turbo function for the 11g wireless network. Make sure your clients also support this function before you enable it.

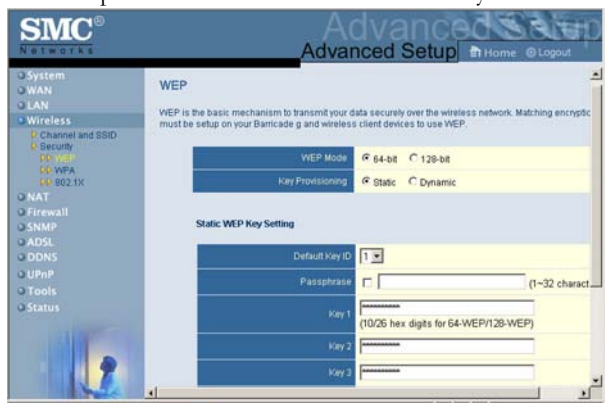
## Security

To make your wireless network safe, you should turn on the security function. The Barricade supports WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected) security mechanisms.



WEP

If you want to use WEP to protect your wireless network, you need to set the same parameters for the Barricade and all your wireless clients.



Parameter	Description
WEP Mode	Select 64 bit or 128 bit key to use for encryption.
Key Provisioning	Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you would need to enable 802.1X function first.

You may automatically generate encryption keys or manually enter the keys. To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop down menu. Click “APPLY”.

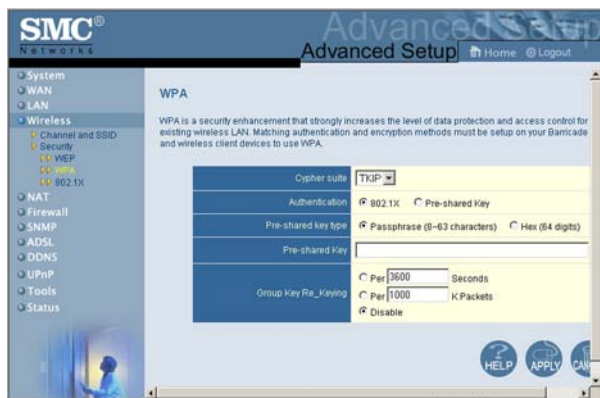
**Note:** The passphrase can consist of up to 32 alphanumeric characters.

To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F)

Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

## WPA

Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1X mechanisms. It provides dynamic key encryption and 802.1X authentication service.

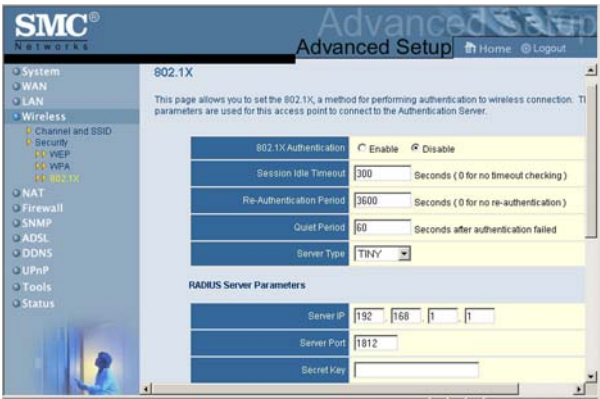


Parameter	Description
Cypher suite	The security mechanism used in WPA for encryption.
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. <ul style="list-style-type: none"> <li>•802.1X: for the enterprise network with a RADIUS server.</li> <li>•Pre-shared key: for the SOHO network environment without an authentication server.</li> </ul>
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type in the key here.
Group Key Re-Keying	The period of renewing broadcast/multicast key.



802.1X

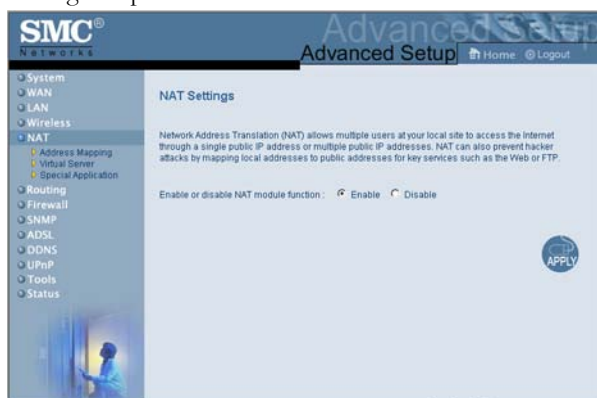
If 802.1X is used in your network, then you should enable this function for the Barricade.



Parameter	Description
802.1X Authentication	Enable or disable this authentication function.
Session Idle timeout	Defines a maximum period of time for which the connection is maintained during inactivity.
Re-Authentication Period	Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client.
Quiet Period	Defines a maximum period of time for which the Barricade will wait between failed authentications.
Server Type	Select TINY or RADIUS as the authentication server.
RADIUS Server Parameters	
Server IP	The IP address of your authentication server.
Server Port	The port used for the authentication service.
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	Defines the request identifier of the Network Access Server.

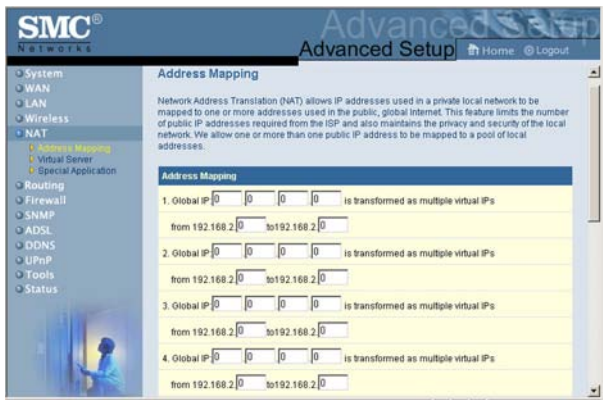
## NAT

Network Address Translation allows multiple users to access the Internet sharing one public IP.



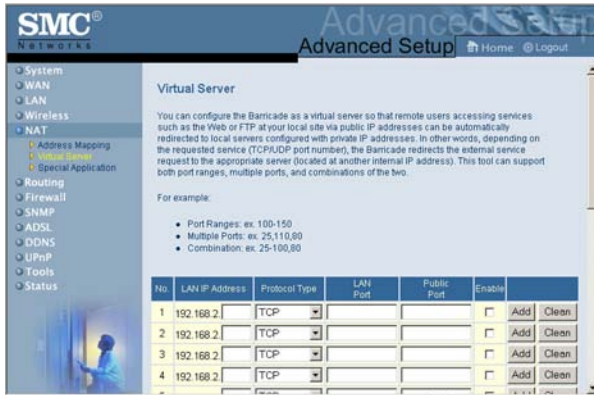
Address Mapping

Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP into the “from” field.



## Virtual Server

If you configure the Barricade as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Barricade redirects the external service request to the appropriate server (located at another internal IP address).



For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

The more common TCP service ports include:

HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110. A list of ports is maintained at the following link:

<http://www.iana.org/assignments/port-numbers>.

**Note:** The WAN interface should have a fixed IP address to best utilize this function. See “DDNS” on page 4-57 for using the same domain name even though your IP address changes each time you log into the ISP.

Special Application

Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony. These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these pages to specify the additional public ports to be opened for each application.

SMC<sup>®</sup>  
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Address Mapping

Virtual Server

Special Application

Routing

Firewall

SNMP

ADSL

DDNS

UPnP

Tools

Status

Special Applications

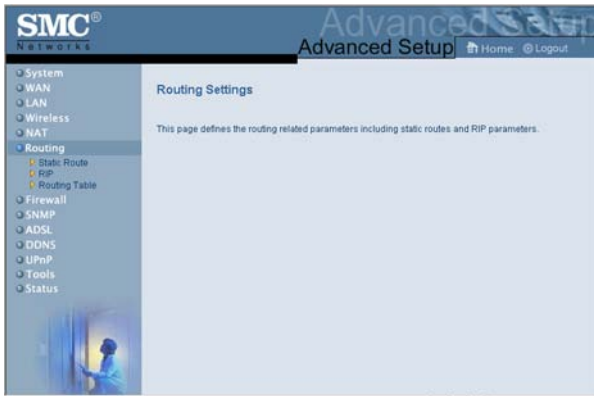
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Note: The range of the Trigger Ports is from 1 to 65535.

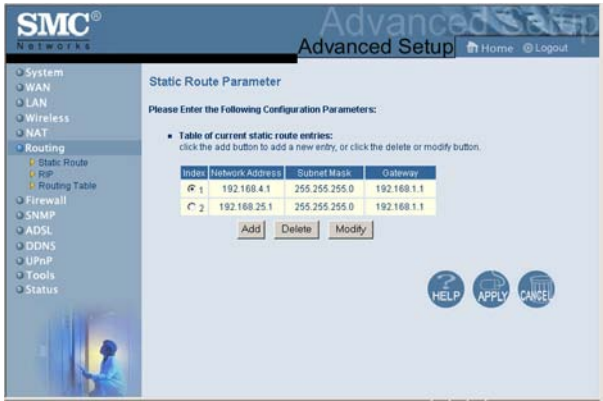
	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

## Routing

These pages define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.



Static Route



Parameter	Description
Index	Check the box of the route you wish to delete or modify.
Network Address	Enter the IP address of the remote computer for which to set a static route.
Subnet Mask	Enter the subnet mask of the remote network for which to set a static route.
Gateway	Enter the WAN IP address of the gateway to the remote network.

Click “Add” to add a new static route to the list, or check the box of an already entered route and click “Modify”. Clicking “Delete” will remove an entry from the list.

## RIP

Parameter	Description
-----------	-------------

## General RIP Parameters

RIP mode	Globally enables or disables RIP.
Auto summary	If Auto summary is disabled, then RIP packets will include sub-network information from all sub-networks connected to the router. If enabled, this sub-network information will be summarized to one piece of information covering all sub-networks.

## Table of current Interface RIP parameter

Interface	The WAN interface to be configured.
Operation Mode	Disable: RIP disabled on this interface. Enable: RIP enabled on this interface. Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts.
Version	Sets the RIP (Routing Information Protocol) version to use on this interface.
Poison Reverse	A method for preventing loops that would cause endless retransmission of data traffic.



Parameter	Description
Authentication Required	<ul style="list-style-type: none"><li>• None: No authentication.</li><li>• Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets.</li><li>• MD5: An algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.</li></ul>
Authentication Code	Password or MD5 Authentication key.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.

## Routing Table




---

Parameter	Description
-----------	-------------

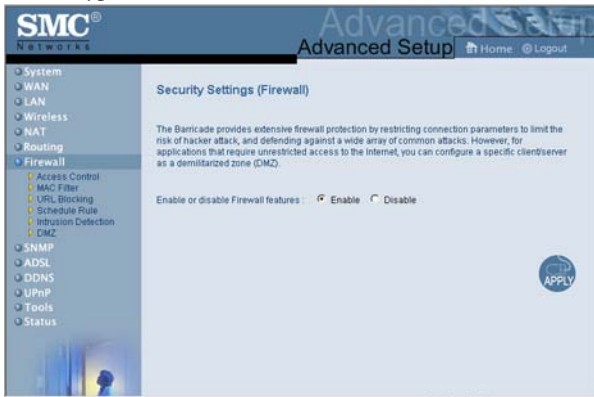
---

Flags	<p>Indicates the route status:</p> <p>C = Direct connection on the same subnet.</p> <p>S = Static route.</p> <p>R = RIP (Routing Information Protocol) assigned route.</p> <p>I = ICMP (Internet Control Message Protocol) Redirect route.</p>
Network Address	Destination IP address.
Netmask	<p>The subnetwork associated with the destination.</p> <p>This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the subnet mask number; each bit that corresponds to “0” is part of the host number.</p>
Gateway	The IP address of the router at the next hop to which frames are forwarded.
Interface	The local interface through which the next hop of this route is reached.
Metric	When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

---

## Firewall

The Barricade Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.



Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (See page 4-46 for details.)

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network. Select Enable and click the “APPLY” button to open the Firewall submenus.

## Access Control

Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.



The following items are on the Access Control screen:

Parameter	Description
Enable Filtering Function	Click Yes to turn on the filtering function.
Normal Filtering Table	Displays the IP address (or an IP address range) filtering table.

To add the PC to the filtering table:

- 1. Click “Add PC” on the Access Control screen.
- 2. Define the appropriate settings for client PC services.
- 3. Click “OK” and then click “APPLY” to save your settings.



## MAC Filter

The Barricade can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the Barricade to enter up to 32 MAC addresses that are not allowed access to the WAN port.

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Routing, Firewall (selected), Access Control, MAC Filter (selected), URL Blocking, Schedule Rule, Intrusion Detection, DMZ, SNMP, ADSL, DDNS, UPnP, Tools, and Status. The main content area is titled 'MAC Filtering Table'. It includes a description: 'This section helps provides MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients.' Below this are two options: 'MAC Address Control:' with radio buttons for 'Yes' (selected) and 'No', and 'MAC Filtering Table (up to 32 computers)'.

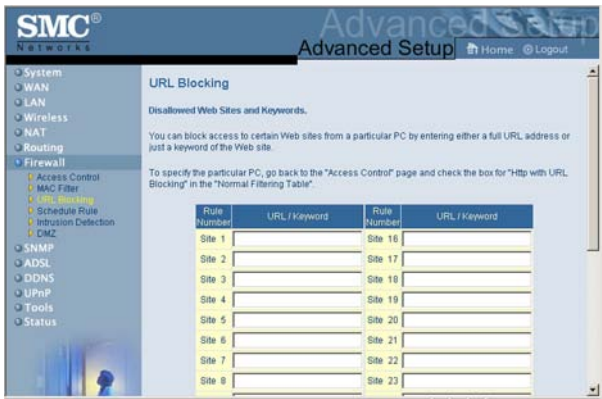
ID	MAC Address					
1	:	:	:	:	:	:
2	:	:	:	:	:	:
3	:	:	:	:	:	:
4	:	:	:	:	:	:
5	:	:	:	:	:	:
6	:	:	:	:	:	:
7	:	:	:	:	:	:
8	-	-	-	-	-	-

Click Yes to enable, or No to disable this function.

Enter the MAC address in the space provided.

URL Blocking

The Barricade allows the user to block access to web sites from a particular PC by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.



You can define up to 30 sites here.

## Schedule Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the Schedule Rule page, and apply the rule on the Access Control page.



Follow these steps to add a schedule rule:

1. Click “Add Schedule Rule”.
2. Define the appropriate settings for a schedule rule (as shown in this example).
3. Click “OK” and then click “APPLY” to save your settings.

**Edit Schedule Rule**

Name:

Comment:

Activate Time Period:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>
Sunday	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>
Monday	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>
Tuesday	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>
Wednesday	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>
Thursday	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>
Friday	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>
Saturday	<input type="text" value="08"/> : <input type="text" value="30"/>	<input type="text" value="18"/> : <input type="text" value="00"/>



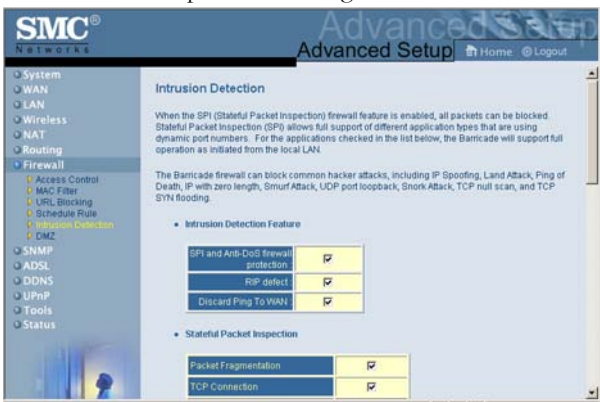
**Intrusion Detection**

- Intrusion Detection Feature**

Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) — The Intrusion Detection Feature of the Barricade Router limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the Stateful Packet Inspection section.

RIP Defect (Default: Enabled) — If an RIP request packet is not acknowledged to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets from accumulating.

Discard Ping to WAN (Default: Disabled) — Prevent a ping on the Barricade’s WAN port from being routed to the network.



Scroll down to view more information.

**SMC® NETWORKS**

**Advanced Setup** Home Logout

- When hackers attempt to enter your network, we can alert you by e-mail
  - Your E-mail Address
  - SMTP Server Address
  - POP3 Server Address
  - User name
  - Password
- Connection Policy
  - Fragmentation half-open wait  sec
  - TCP SYN wait  sec
  - TCP FIN wait  sec
  - TCP connection idle timeout  sec
  - UDP session idle timeout  sec
  - H.323 data channel idle timeout  sec
- DoS Detect Criteria:
  - Total incomplete TCP/UDP sessions HIGH  session

- **Stateful Packet Inspection**

This is called a “stateful” packet inspection because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks “FTP Service” in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

Stateful Packet Inspection allows you to select different application types that are using dynamic port numbers. If you wish to use the Stateful Packet Inspection (SPI) to block packets, click on the Yes radio button in the

“Enable SPI and Anti-DoS firewall protection” field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, or TFTP Service.

- **When hackers attempt to enter your network, we can alert you by e-mail**

Enter your email address. Specify your SMTP and POP3 servers, user name, and password.

- **Connection Policy**

Enter the appropriate values for TCP/UDP sessions as described in the following table.

Parameter	Defaults	Description
Fragmentation half-open wait	10 sec	Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet.
TCP SYN wait	30 sec	Defines how long the software will wait for a TCP session to synchronize before dropping the session.
TCP FIN wait	5 sec	Specifies how long a TCP session will be maintained after the firewall detects a FIN packet.
TCP connection idle timeout	3600 seconds (1 hour)	The length of time for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 sec	The length of time for which a UDP session will be managed if there is no activity.
H.323 data channel idle timeout	180 sec	The length of time for which an H.323 session will be managed if there is no activity.

- **DoS Criteria and Port Scan Criteria**

Set up DoS and port scan criteria in the spaces provided (as shown below).

Parameter	Defaults	Description
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of new unestablished sessions that will cause the software to <i>start</i> deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to <i>stop</i> deleting half-open sessions.
Incomplete TCP/UDP sessions (per min) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/UDP sessions (per min) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute.
Maximum incomplete TCP/UDP sessions number from same host	10	Maximum number of incomplete TCP/UDP sessions from the same host.
Incomplete TCP/UDP sessions detect sensitive time period	300 msec	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	10000 msec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 second	Length of time from detecting a flood attack to blocking the attack.

**Note:** The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.

DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.



## SNMP

Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP).

### Community

A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Barricade, the NMS must first submit a valid community string for authentication.

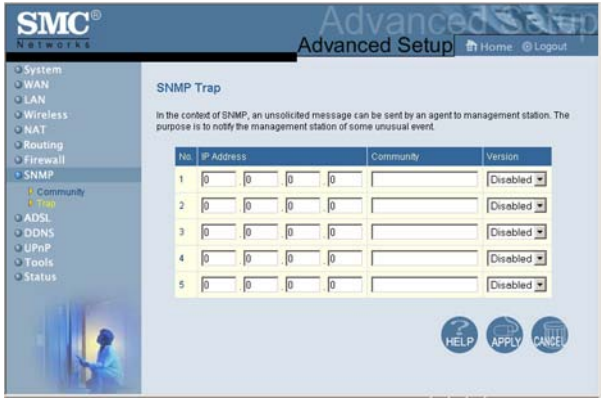


Parameter	Description
Community	A community name authorized for management access.
Access	Management access is restricted to Read Only (Read) or Read/Write (Write).
Valid	Enables/disables the entry.

**Note:** Up to five community names may be entered.

Trap

Specify the IP address of the NMS to notify when a significant event is detected by the agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMS specified as a trap receiver.



Parameter	Description
IP Address	Traps are sent to this address when errors or specific events occur on the network.
Community	A community string (password) specified for trap management. Enter a word, something other than public or private, to prevent unauthorized individuals from accessing information on your system.
Version	Sets the trap status to disabled, or enabled with V1 or V2c.  The v2c protocol was proposed in late 1995 and includes enhancements to v1 that are universally accepted. These include a get-bulk command to reduce network management traffic when retrieving a sequence of MIB variables, and a more elaborate set of error codes for improved reporting to a Network Management Station.

## ADSL

ADSL (Asymmetric Digital Subscriber Line) is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream. This section is used to configure the ADSL operation type and shows the ADSL status.

### Parameters

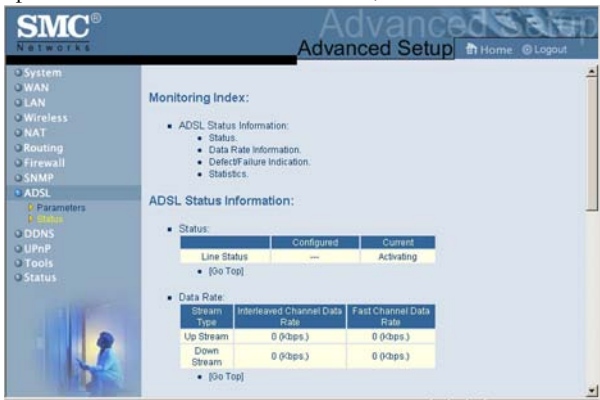


Parameter	Description
Operation Mode	<ul style="list-style-type: none"> <li>Automatic</li> <li>T1.413 issue 2</li> <li>G.992.1</li> <li>G.992.2</li> </ul>
Address C3, etc.	Reserved

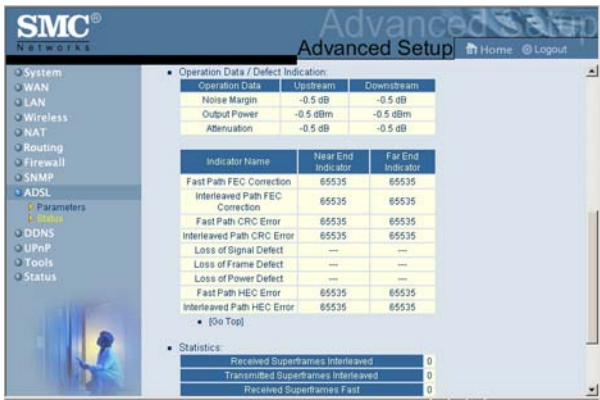


Status

The Status screen displays information on connection line status, data rate, operation data and defect indication, and statistics.



Scroll down to view more information.



The following items are included on this information page:

Parameter	Description
Status	
Line Status	Shows the current status of the ADSL line connection.
Data Rate	
Upstream	Maximum upstream data rate.
Downstream	Maximum downstream data rate.
Operation Data/Defect Indication	
Noise Margin	Maximum upstream and downstream noise margin.
Output Power	Maximum fluctuation in the output power.
Attenuation	Maximum reduction in the strength of the upstream and downstream signal.
Fast Path FEC Correction	There are two latency paths that may be used: fast and interleaved. For either path, a forward error correction (FEC) scheme is employed to ensure higher data integrity. For maximum noise immunity, an interleaver may be used to supplement FEC.
Interleaved Path FEC Correction	An interleaver is basically a buffer used to introduce a delay, allowing for additional error correction techniques to handle noise. Interleaving slows the data flow and may not be optimal for real-time signals such as video transmission.
Fast Path CRC Error	The number of Fast Path Cyclic Redundancy Check errors.
Interleaved Path CRC Error	The number of Interleaved Path Cyclic Redundancy Check errors.
Loss of Signal Defect	Momentary signal discontinuities.
Loss of Frame Defect	Failures due to loss of frames.
Loss of Power Defect	Failures due to loss of power.
Fast Path HEC Error	Fast Path Header Error Concealment errors.
Interleaved Path HEC Error	Interleaved Path Header Error Concealment errors.

Parameter	Description
Statistics	(Superframes represent the highest level of data presentation. Each superframe contains regular ADSL frames, one of which is used to provide superframe synchronization, identifying the start of a superframe. Some of the remaining frames are also used for special functions.)
Received Superframes Interleaved	Number of interleaved superframes received.
Transmitted Superframes Interleaved	Number of interleaved superframes transmitted.
Received Superframes Fast	Number of fast superframes received.
Transmitted Superframes Fast	Number of fast superframes transmitted.

## DDNS

Dynamic Domain Name Service (DDNS) provides users on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

This DNS feature is powered by TZO.com. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address.

**SMC**  
Routers

Advanced Setup | Home | Logout

DDNS (Dynamic DNS) Settings

DDNS allows users to map a static Domain Name to a dynamic IP address. However, You must get an account, password, and your static Domain Name from a DDNS service provider. This router supports DDNS services from [www.dyndns.org](http://www.dyndns.org) and [www.tzo.com](http://www.tzo.com).

Dynamic DNS: ☒ Enable ☐ Disable

Provider: TZO.com

Domain Name:

Account / E-mail:

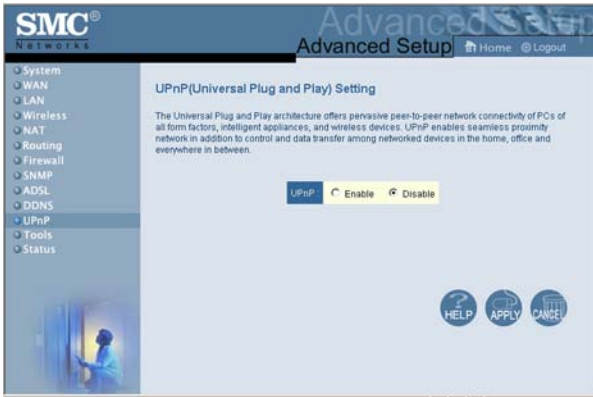
Password / Key:

HELP APPLY CANCEL

## UPnP

Click Enable to turn on the Universal Plug and Play function of the Barricade. This function allows the device to automatically:

- dynamically join a network
- obtain an IP address

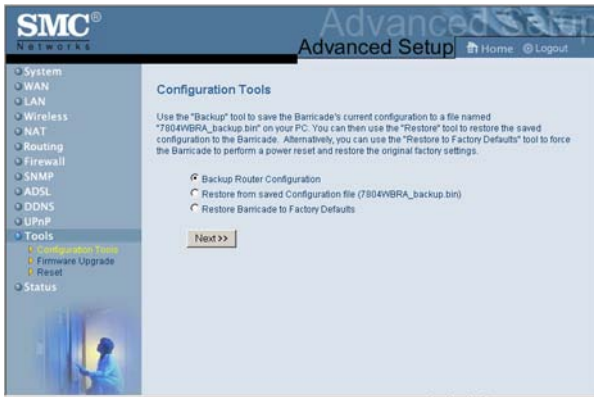


## Tools

Use the Tools menu to backup the current configuration, restore a previously saved configuration, restore factory settings, update firmware, and reset the Barricade.

### Configuration Tools

Choose a function and click Next.



Backup allows you to save the Barricade Router's configuration to a file. Restore can be used to restore the saved backup configuration file. Restore to Factory Defaults resets the Barricade to the original settings.

You will be asked to confirm your decision.

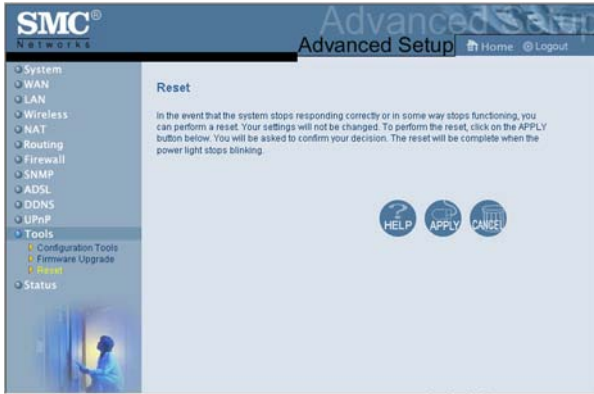
## Firmware Upgrade

Use this screen to update the firmware or user interface to the latest versions. Download the upgrade file from the SMC web site, and save it to your hard drive. In the Upgrade Target field, choose Firmware. Then click “Browse...” to look for the downloaded file. Click “APPLY”. Check the Status page Information section to confirm that the upgrade process was successful.



## Reset

Click “APPLY” to reset the Barricade. The reset will be complete when the power LED stops blinking.



If you perform a reset from this page, the configurations will not be changed back to the factory default settings.

**Note:** If you use the Reset button on the front panel, the Barricade performs a power reset. If the button is depressed for over five seconds, all the LEDs will illuminate and the factory settings will be restored.

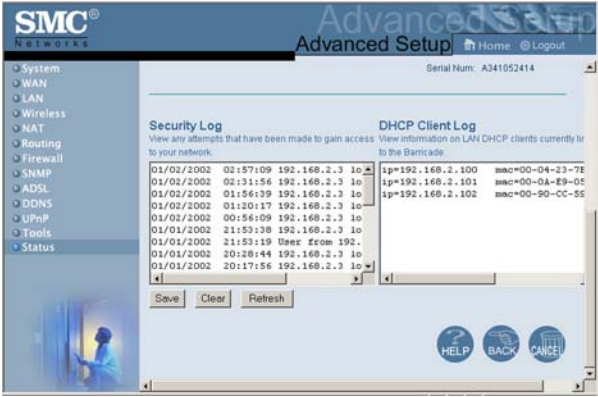


Status

The Status page displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network. The security log may be saved to a file by clicking “Save” and choosing a location.



Scroll down to view more information on the Status page.



The following items are included on the Status page:

Item	Description
INTERNET	Displays WAN connection type and status. Click the Connect button to connect to your ISP.
GATEWAY	Displays system IP settings, as well as DHCP Server and Firewall status.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and for the Barricade, as well as the hardware version and serial number.
Security Log	Displays illegal attempts to access your network.
Save	Click on this button to save the security log file.
Clear	Click on this button to delete the access log.
Refresh	Click on this button to refresh the screen.
DHCP Client Log	Displays information on DHCP clients on your network.

## Finding the MAC address of a Network Card

### Windows 98/ME

Click Start/Run. Type “winipcfg” and press “ENTER”.

The MAC address is in the “Adapter Address” section.

### Windows NT4/2000/XP

Click Start/Programs/Command Prompt. Type “ipconfig /all” and press “ENTER”.

The MAC address is listed as the “Physical Address.”

### Macintosh

Click System Preferences/Network.

The MAC address is listed as the “Ethernet Address” on the TCP/IP tab.

### Linux

Run the command “/sbin/ifconfig.”

The MAC address is the value after the word “HWaddr.”

# APPENDIX A

## TROUBLESHOOTING

---

This section describes common problems you may encounter and possible solutions to them. The Barricade can be easily monitored through panel indicators to identify problems.

Troubleshooting Chart	
Symptom	Action
LED Indicators	
Power LED is Off	<ul style="list-style-type: none"><li>• Check connections between the Barricade, the external power supply, and the wall outlet.</li><li>• If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet.</li></ul> <p>If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.</p>

Troubleshooting Chart	
Symptom	Action
LED Indicators	
Link LED is Off	<ul style="list-style-type: none"> <li>Verify that the Barricade and attached device are powered on.</li> <li>Be sure the cable is plugged into both the Barricade and the corresponding device.</li> <li>Verify that the proper cable type is used and that its length does not exceed the specified limits.</li> <li>Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode.</li> <li>Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.</li> </ul>
Network Connection Problems	
Cannot ping the Barricade from the attached LAN	<ul style="list-style-type: none"> <li>Verify that the IP addresses are properly configured. For most applications, you should use the Barricade's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Barricade and any attached LAN devices.</li> <li>Be sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP.</li> </ul>

Troubleshooting Chart	
Symptom	Action
Management Problems	
Cannot connect using the web browser	<ul style="list-style-type: none"><li>• Be sure to have configured the Barricade with a valid IP address, subnet mask, and default gateway.</li><li>• Check that you have a valid network connection to the Barricade and that the port you are using has not been disabled.</li><li>• Check the network cabling between the management station and the Barricade.</li></ul>
Forgot or lost the password	<ul style="list-style-type: none"><li>• Press the Reset button on the rear panel (holding it down for at least five seconds) to restore the factory defaults.</li></ul>

Troubleshooting Chart	
Symptom	Action
Wireless Problems	
A wireless PC cannot associate with the Barricade.	<ul style="list-style-type: none"> <li>• Make sure the wireless PC has the same SSID settings as the Barricade. See “Channel and SSID” on page 4-26.</li> <li>• You need to have the same security settings on the clients and the Barricade. See “Security” on page 4-27.</li> </ul>
The wireless network is often interrupted.	<ul style="list-style-type: none"> <li>• Move your wireless PC closer to the Barricade to find a better signal. If the signal is still weak, change the angle of the antenna.</li> <li>• There may be interference, possibly caused by a microwave ovens or wireless phones. Change the location of the interference sources or of the Barricade.</li> <li>• Change the wireless channel on the Barricade. See “Channel and SSID” on page 4-26.</li> <li>• Check that the antenna, connectors, and cabling are firmly connected.</li> </ul>
The Barricade cannot be detected by a wireless client.	<ul style="list-style-type: none"> <li>• The distance between the Barricade and wireless PC is too great.</li> <li>• Make sure the wireless PC has the same SSID and security settings as the Barricade. See Barricade. See “Channel and SSID” on page 4-26 and “Security” on page 4-27.</li> </ul>

# APPENDIX B

## CABLES

---

### Ethernet Cable

**Caution:** DO NOT plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

### Specifications

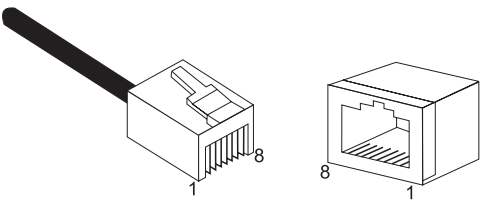
Cable Types and Specifications			
Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45

### Wiring Conventions

For Ethernet connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.



Each wire pair must be attached to the RJ-45 connectors in a specific orientation. The following figure illustrates how the pins on an Ethernet RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



**Figure B-1. RJ-45 Ethernet Connector Pin Numbers**

**RJ-45 Port Connection**

Use the straight-through CAT-5 Ethernet cable provided in the package to connect the Barricade to your PC. When connecting to other network devices such as an Ethernet switch, use the cable type shown in the following table.

Attached Device Port Type	Connecting Cable Type
MDI-X	Straight-through
MDI	Crossover

Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

RJ-45 Pin Assignments	
Pin Number	Assignment <sup>1</sup>
1	Tx+
2	Tx-
3	Rx+
6	Rx-

1: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

If the port on the attached device has internal crossover wiring (MDI-X), then use straight-through cable.

Straight-Through Cable Pin Assignments	
End 1	End 2
1 (Tx+)	1 (Tx+)
2 (Tx-)	2 (Tx-)
3 (Rx+)	3 (Rx+)
6 (Rx-)	6 (Rx-)

**Crossover Wiring**

If the port on the attached device has straight-through wiring (MDI), use crossover cable.

Crossover Cable Pin Assignments	
End 1	End 2
1 (Tx+)	3 (Rx+)
2 (Tx-)	6 (Rx-)
3 (Rx+)	1 (Tx+)
6 (Rx-)	2 (Tx-)

# ADSL Cable

Use standard telephone cable to connect the RJ-11 telephone wall outlet to the RJ-45 ADSL port on the ADSL Router.

**Caution:** Do not plug a phone jack connector into an RJ-45 port.

## Specifications

Cable Types and Specifications		
Cable	Type	Connector
ADSL Line	Standard Telephone Cable	RJ-11

## Wiring Conventions

For ADSL connections, a cable requires one pair of wires. Each wire is identified by different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-11 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-11 connectors in a specific orientation. The following figure illustrates how the pins on the RJ-11 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

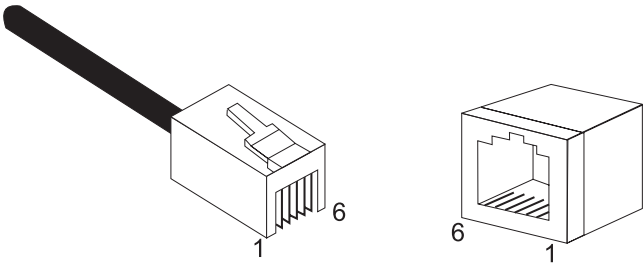
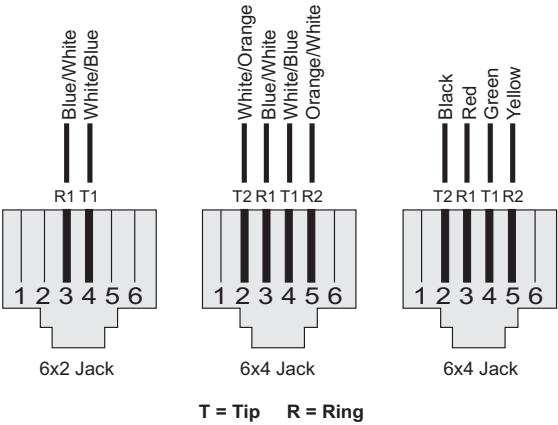


Figure B-2. RJ-11 Connector Pin Numbers



Pin	Signal Name	Wire Color
1	Not used	
2	Line 2 Tip	Black or White/Orange
3	Line 1 Ring	Red or Blue/White
4	Line 1 Tip	Green or White/Blue
5	Line 2 Ring	Yellow or Orange/White
6	Not used	

Figure B-3. RJ-11 Pinouts

# APPENDIX C

## SPECIFICATIONS

---

### **Physical Characteristics**

#### **Ports**

Four 10/100Mbps RJ45 Ports

One ADSL RJ11

Two external dipole antennas

#### **ADSL Features**

Supports DMT line modulation

Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 & T1.413, Issue 2)

Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps upstream

Dying GASP support

#### **ATM Features**

RFC1483 Encapsulation (IP, Bridging and encapsulated routing)

PPP over ATM (LLC & VC multiplexing) (RFC2364)

Classical IP (RFC1577)

Traffic shaping (UBR, CBR)

OAM F4/F5 support

PPP over Ethernet Client

#### **Management Features**

Firmware upgrade via WEB Based Management

WEB Based Management (configuration)

Power Indicators

Event and History logging

Network Ping

**Security Features**

Password protected configuration access

User authentication (PAP/CHAP) with PPP

Firewall NAT NAPT

VPN pass through (IPSec-ESP Tunnel mode,L2TP, PPTP)

**LAN Features**

IEEE 802.1D (self-learning transparent Bridging)

DHCP Server

DNS Proxy

Static Routing, RIPv1 and RIP

**Applications**

Netmeeting, ICQ, Real Player, QuickTime, DialPad, PC Anywhere, Telnet,  
SNTP, NNTP

**Radio Features**

**Wireless RF module Frequency Band**

802.11g Radio: 2.4GHz

802.11b Radio: 2.4GHz

USA - FCC

2412~2462MHz (Ch1~Ch11)

Canada - IC

2412~2462MHz (Ch1~Ch11)

Europe - ETSI

2412~2472MHz (Ch1~Ch13)

Spain

2457~2462MHz (Ch10~Ch11)

France

2457~2472MHz (Ch10~Ch13)

Japan - STD-T66/STD-33

2412~2484MHz (Ch1~Ch14)

**Modulation Type**

OFDM, CCK

**Operating Channels IEEE 802.11b compliant:**

11 channels (US, Canada)

13 channels (ETSI)

2 Channels (Spain)

4 Channels (France)

14 channels (Japan)

**Operating Channels IEEE 802.11g compliant:**

13 channels (US, Canada, Europe, Japan)

**RF Output Power Modulation Rate-Output Power (dBm)**

802.11b - 1Mbps 16

802.11b - 2Mbps 16

802.11b - 5.5Mbps 16

802.11b - 11Mbps 16

**Modulation Rate-Output Power (dBm)**

802.11g - 6Mbps 15

802.11g - 9Mbps 15

802.11g - 12Mbps 15

802.11g - 18Mbps 15

802.11g- 24Mbps 15

802.11g - 36Mbps 15

802.11g- 48Mbps 15

802.11g - 54Mbps 15

**Sensitivity Modulation Rate-Receiver 2.412 ~ 2.484 HGz Sensitivity  
(dBm)**

802.11b - 1Mbps -90

802.11b - 2Mbps -88

802.11b - 5.5Mbps -85

802.11b- 11Mbps -84



**Modulation Rate-Receiver Sensitivity Typical (dBm)**

802.11g - 6Mbps -88

802.11g - 9Mbps -87

802.11g - 12Mbps -84

802.11g - 18Mbps -82

802.11g - 24Mbps -79

802.11g - 36Mbps -75

802.11g - 48Mbps -68

802.11g - 54Mbps -68

**Environmental**

SMC7804WBRA complies with the following standards:

**Temperature: IEC 68-2-14**

0 to 50 degrees C (Standard Operating)

-40 to 70 degree C (Non-operation)

**Humidity**

10% to 90% (Non-condensing)

**Vibration: IEC 68-2-36, IEC 68-2-6**

**Shock: IEC 68-2-29**

**Drop: IEC 68-2-32**

**Dimensions**

220 x 132 x 30 (mm)

**Weight**

550 g

**Input Power**

12 V 1 A

**IEEE Standards**

IEEE 802.3, 802.3u, 802.11g, 802.1D

ITU G.dmt

ITU G.Handshake

ITU T.413 issue 2 - ADSL full rate

**Standards Conformance Electromagnetic Compatibility**

CE, ETSI, R&TTE, FCC part 15 class B & FCC part 68, ETS 300 328,  
ETS 300 826

**Safety**

CSA/NRTL (UL1950, CSA 22.2.950) GS (EN60950), CB (IEC60950)

**Internet Standards**

RFC 826 ARP

RFC 791 IP

RFC 792 ICMP

RFC 768 UDP

RFC 793 TCP

RFC 783 TFTP

RFC 1483 AAL5 Encapsulation

RFC 1661 PPP

RFC 1866 HTML

RFC 2068 HTTP

RFC 2364 PPP over ATM

## *SPECIFICATIONS*

#### FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)

(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481

From Europe: Contact details can be found on

[www.smc-europe.com](http://www.smc-europe.com) or [www.smc.com](http://www.smc.com)

#### INTERNET

E-mail addresses:

[techsupport@smc.com](mailto:techsupport@smc.com)

[european.techsupport@smc-europe.com](mailto:european.techsupport@smc-europe.com)

Driver updates:

[http://www.smc.com/index.cfm?action=tech\\_support\\_drivers\\_downloads](http://www.smc.com/index.cfm?action=tech_support_drivers_downloads)

World Wide Web:

<http://www.smc.com/>

<http://www.smc-europe.com/>

#### For Literature or Advertising Response, Call:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-91-352-00-40	Fax 34-93-477-3774
UK:	44 (0) 8712 779802	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 3355708602	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920	Fax 34 93 477 3774
Sub Saharan Africa:	216-712-36616	Fax 216-71751415
North West Africa:	34 93 477 4920	Fax 34 93 477 3774
CIS:	7 (095) 7893573	Fax 7 (095) 789 357
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-87978006	Fax 886-2-87976288
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-45-224-2332	Fax 81-45-224-2331
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

If you are looking for further contact information, please visit [www.smc.com](http://www.smc.com) or [www.smc-europe.com](http://www.smc-europe.com).

**SMC**<sup>®</sup>  
Networks

38 Tesla  
Irvine, CA 90618  
Phone: (949) 679-8000